ASSISTANT COMMISSIONER OF PATENTS
Box: New Application
Washington, D.C. 20231

JC820 U.S. PTO
09/19/00

Sir:

Docket No. 30604

Date September 14, 2000

JC658 U.S. PTO
09/664093
09/19/00

Transmitted herewith for filing under 35 U.S.C. 111 and 37. C.F.R. 1.53 is the patent application of:

INVENTOR(S): JOHN EVERSON, and JAMES W. NORRIS

FOR: AUTHENTICATION, APPLICATION-AUTHORIZATION, AND USER PROFILING USING DYNAMIC DIRECTORY SERVICES

Enclosed are:

X Certificate of Mailing with Express Mail Mailing Label No. EL618532394US

X 1 sheets of drawing(s)

X Combined Declaration and Power of Attorney

X An Assignment of the invention to SPRINT SPECTRUM, L.P. together with the recording fee of $40.00.

___ A verified statement to establish small entity status under 37 CFR 1.9 and 37 CFR 1.27.

___ Information Disclosure Statement

The filing fee has been calculated as shown below:

	(Col. 1)	(Col. 2)	SMALL ENTITY			OTHER THAN A SMALL ENTITY	
FOR:	NO. FILED	NO. EXTRA	RATE	FEE	OR	RATE	FEE
BASIC FEE				$ 345.00	OR		$ 690.00
TOTAL CLAIMS	12-20=	* 0	x 9		OR	x 18	
INDEP. CLAIMS	2-3=	* 0	x 39		OR	x 78	
MULTIPLE DEPENDENT CLAIM PRESENT			+130		OR	+260	
*If the difference in col. 1 is less than zero, enter "0" in Col. 2			TOTAL	$	OR	TOTAL	$690.00

___ Please charge my Deposit Account No. 19-0522 in the amount of $ _____. A duplicate of this sheet is enclosed.

X A check in the amount of $690.00 to cover the filing fee is enclosed.

X The Commissioner is hereby authorized to charge payment of the following fees associated with this communication or credit any overpayment to Deposit Account No. 19-0522. A duplicate of this sheet is enclosed.

X Any additional filing fees required under 37 CFR 1.16.

X Any patent application processing fees under 37 CFR 1.17.

X The Commissioner is hereby authorized to charge payment of the following fees during the pendency of this application or credit any overpayment to Deposit Account No. 19-0522. A duplicate copy of this sheet is enclosed.

X Any patent application processing fees under 37 CFR 1.16.

___ The issue fee set in 37 CFR 1.18 at or before the mailing of the Notice of Allowance, pursuant to 37 CFR 1.311(f).

X Any fees under 37 CFR 1.16 for presentation of extra claims.

By _____
Thomas B. Luebbering, Reg. No. 37,874

23589

PATENT TRADEMARK OFFICE

CERTIFICATION UNDER 37 C.F.R. 1.10

Enclosed for filing is the application for United States Letters Patent of JOHN EVERSON and JAMES W. NORRIS, Attorney Docket No. 30604, entitled AUTHENTICATION, APPLICATION-AUTHORIZATION, AND USER PROFILING USING DYNAMIC DIRECTORY SERVICES, including: **Transmittal, Specification, Claims, Abstract, 1 sheet informal drawings, Combined Declaration and Power of Attorney, $690.00 filing fee, Assignment Cover Sheet, Assignment, $40.00 recordation fee, and return card.**

EL618532394US
"Express Mail" mailing number

September 19, 2000
Date of Deposit

I hereby certify that the above-noted papers are being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 C.F.R. 1.10 on the date indicated above and is addressed to BOX NEW APPLICATION, Assistant Commissioner for Patents, Washington, DC 20231.

Heidi Caragan
Name of person mailing

Heidi Caragan
Signature of person mailing

AUTHENTICATION, APPLICATION-AUTHORIZATION, AND USER PROFILING USING DYNAMIC DIRECTORY SERVICES

BACKGROUND OF THE INVENTION

1. FIELD OF THE INVENTION

The present invention relates to the fields of computer authentication, application authorization and user profiling. More particularly, the invention relates to the use of dynamic directory services (DDS) to dynamically store information in a directory server that can be used for authentication, application authorization, and user profiling purposes to eliminate the need for numerous authorization and access control schemes with a single standard directory based set of applications.

2. DESCRIPTION OF THE PRIOR ART

Many computer networks require users to be authenticated before they are allowed access thereto. Similarly, many computer applications and/or programs can only be accessed or used by authorized users. Computer users are typically authenticated and/or authorized by access control and security programs that contain or consult user profiles or databases (data repositories) containing access control information for the users. These access control and security programs typically require the entry of user IDs, passwords, etc., before users are allowed access to the networks and/or programs and applications.

Most networks, programs, and applications that have secured entries have their own proprietary access control and security systems (front and back). This requires computer users who wish to gain access to more than one network, application, and/or program during a computer session to repeatedly re-enter their user IDs, passwords, etc., each time they attempt to transfer from one network to another or from one application or program to another. This also requires each network, application, and program to have and maintain its own separate access control information for all users.

SUMMARY OF THE INVENTION

The present invention solves the above-described problems and provides a distinct advance in the art of computer authentication and authorization. More

particularly, the present invention provides a system and method for authenticating and authorizing computer users with a single, standard, directory-based set of applications.

The present invention combines Dynamic Directory Services (DDS) with a directory access protocol such as the Lightweight Directory Access Protocol (LDAP) to provide authentication and authorization for secured networks, applications, and programs. The present invention uses DDS to store dynamic information such as session information or user ID information in a directory each time a user logs into the system and then maintains the information in the directory until the user logs out. While the information exists in the directory, it can be queried by any other program, application, or network that uses LDAP or other directory protocol to authenticate or authorize the user for the network or application. The present invention therefore eliminates the need to maintain separate access control systems for each secured network, program, or application.

The method and system of the present invention may also be used to provide a more convenient on-line shopping cart and for user profiling and session profiling purposes.

These and other important aspects of the present invention are described more fully in the detailed description below.

BRIEF DESCRIPTION OF THE DRAWING FIGURES

A preferred embodiment of the present invention is described in detail below with reference to the attached drawing figure, wherein:

Fig. 1 is a schematic diagram of computer and communications equipment that may be used to implement certain aspects of a preferred embodiment of the present invention.

The drawing figure does not limit the present invention to the specific embodiments disclosed and described herein. The drawing Figure is not necessarily to scale, emphasis instead being placed upon clearly illustrating the principles of the invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention combines a directory access protocol such as the Lightweight Directory Access Protocol (LDAP) or X.500 with Dynamic Directory Services

(DDS) to provide authentication and application-authorization for secured networks, applications, and programs. Instead of using a directory for static information such as user names, addresses, and phone numbers, however, the present invention uses a directory to store dynamic information such as session information or a shopping cart. When a user logs into the system of the present invention, a user object is created in a directory and remains in the directory until the user logs out of the system. Then, any other applications and/or networks accessed by the computer user during the session may simply query the directory to obtain authorization and authentication information. A simple query to the directory can also indicate how many users are logged into the system at any given moment.

The present invention can be implemented in hardware, software, firmware, or a combination thereof. However, the invention is preferably implemented in software that operates computer and communication equipment such as the equipment identified by the numeral 10 in Fig. 1. The computer and communications equipment broadly includes a plurality of user computers 12, one or more application servers 14, one or more authorization servers 16, one or more user profile databases 18, a directory 20, and a communications network 22. The computer equipment and software illustrated and described herein are merely examples of hardware and software that may be used to implement a preferred embodiment of the present invention and may be replaced with other computer equipment and software without departing from the scope of the present invention.

The user computers 12 are entirely conventional and may be, for example, personal computers or even internet appliances. The user computers are each preferably equipped with a web browser and an internet connection such as a modem, an ISDN or DSL converter, or a cable modem so that they can access web sites on the Internet in a conventional manner.

The application servers 14 are coupled with the user computers 12 via the communications network 22 and are provided for running applications on behalf of the user computers. The application servers may be any computing devices such as network or server computers. The application servers may be used to handle all application operations between the browser-based computers 12 and a company's back end business applications or databases. Because many databases cannot interpret

commands written in HTML, the application servers may serve as translators, allowing computer users to search for information with a browser.

The authorization servers 16 are coupled with the user computers 12 and the application servers 14 via the communications network 22 and are provided for authenticating and authorizing the user computers. The authorization servers may be any computing devices such as network or server computers running Windows NT, Novell Netware, Unix, or any other network operating system. As described in more detail below, the authorization servers may use any means for authenticating and authorizing users such as tokens, certificates, IDs, passwords, and access control measures.

The user profile databases 18 are coupled with the authorization servers 16 via the communications network 22 and are operable for storing certain profile information relating to the users of the user computers 12. The user profile databases may store, for example, user IDs, passwords, access control information such as what applications each computer user is allowed to access, shipping addresses, credit card numbers, information about previous purchases, and any other information useful for authentication, application authorization and user profiling and session profiling/management issues.

The directory 20 is coupled with the authorization servers 16 and the user profile databases 18 via the communications network 22 and is provided for storing directory information used in the present invention as described in more detail below. The directory may reside on any conventional computing device such as one or more network computers or server computers.

The communications network 22 may be a local area network, a wide area network, an intranet, an extranet, the Internet, or any other conventional network or combination of networks. In preferred forms, the user computers 12 may access the authorization servers 16 via the Internet, and the other components of the system 10 communicate via a local or wide area network.

The present invention is fully scalable in that any number of the above described devices of the system 10 can be added as needed. Moreover, none of the devices need to be from a particular vendor, or run on a particular platform. For example, there may be five different authorization servers 16 that perform authentication

and authorization of users, but each server may use a different method to authenticate users.

Operation of the computer and communications equipment 10 is controlled by one or more computer programs. Each computer program preferably comprises an ordered listing of executable instructions for implementing logical functions in the authorization servers 16 and the other computing devices as described herein. The computer programs can be embodied in any computer-readable medium for use by or in connection with an instruction execution system, apparatus, or device, such as a computer-based system, processor-containing system, or other system that can fetch the instructions from the instruction execution system, apparatus, or device, and execute the instructions. In the context of this application, a "computer-readable medium" can be any means that can contain, store, communicate, propagate or transport the program for use by or in connection with the instruction execution system, apparatus, or device. The computer-readable medium can be, for example, but not limited to, an electronic, magnetic, optical, electro-magnetic, infrared, or semi-conductor system, apparatus, device, or propagation medium. More specific, although not inclusive, examples of the computer-readable medium would include the following: an electrical connection having one or more wires, a portable computer diskette, a random access memory (RAM), a read-only memory (ROM), an erasable, programmable, read-only memory (EPROM or Flash memory), an optical fiber, and a portable compact disk read-only memory (CDROM). The computer-readable medium could even be paper or another suitable medium upon which the program is printed, as the program can be electronically captured, via for instance, optical scanning of the paper or other medium, then compiled, interpreted, or otherwise processed in a suitable manner, if necessary, and then stored in a computer memory.

The following is a description of the operation of a preferred implementation of the present invention. In some alternative implementations, the functions described below in a particular order may occur out of the order described. For example, two steps described separately may in fact be executed substantially concurrently, or may sometimes be executed in the reverse order depending upon the functionality involved.

A user first launches some application or program in a conventional manner with one of the user computers 12. The particular application or program that

is launched is not important to the present invention and may include, for example, an internet browser, a Java application, a Java applet, a visual basic application, or any other program or application.

The application is initially directed to one of the authorization servers 16. Which authorization server that is accessed may be based on any criteria including, but not limited to, the first authorization server that answers, a round-robin selection process, geographical criteria, or requirements based on the software or application being used.

The user next logs into the selected authorization server 16 using account or ID information that was established during a user-enrollment/setup process that occurred sometime in the past. The type of account information and authentication or authorization may be specific to the type of applications or network that the user has access to or the role that the user has been assigned.

In accordance with one important aspect of the present invention, the authorization server 16 creates a Session ID for the user after log-in. The Session ID may relate to the date or time that the user logged in, the media access control address of the user's computer 12, the TCP/IP address of the user's computer, the user's name, an account code for the user, a combination of any of these criteria, or any other criteria. It is important only that the Session ID be unique to the user and the particular authorization server 16 that was accessed.

The authorization server 16 then copies or links the Session ID or some derivative thereof to something on the user's computer 12 such as a cookie, shared application memory, or the computer's network address. It is important only that other applications launched by the user from the user computer be able to read or otherwise determine this Session ID by accessing something on the user's computer.

The authorization server 16 also creates an object representing the user or the Session ID and stores it in the directory 20 after log-in. The object name is preferably the same as the Session ID but may be any name relating to the Session ID. After the object is created and stored in the directory, the authorization server copies or parses information about the user from the user profile database 18 and writes this information to the new directory object. The type of information depends on who the user is, what applications the user is allowed to use, what the role of the user is, and how the user was authenticated. The information could even include user IDs and

passwords for other applications to provide single log-in or sign-on capabilities. The information may also be encrypted, signed, or otherwise protected for security purposes.

After the user has successfully logged in, the menu or interface of the application the user attempted to launch is loaded so that the user may use the launched application. This function may be performed by the authorization server 16, one of the application servers 14, or any other piece of computer equipment.

The above steps provide a means to authenticate and/or authorize the user for other applications and/or networks. Specifically, when the user attempts to access other applications and/or networks while he or she is still logged into the system, these other applications may reference the Session ID on the user's computer. Using the Session ID, the other applications may read the user information that has been copied to the user's object in the directory for authentication and authorization purposes related to the new applications. The new applications may also be able to modify the information in the object so that the object could pass information to other applications such as in a shopping cart environment described below.

The present invention may be used to replace numerous authorization and access control schemes with one standard, directory-based set of applications. The present invention allows all applications, computer programs, and networks that use a directory access protocol such as LDAP to access all user profile and access control information created for a user while the user is logged into the system. This eliminates the need to create and maintain numerous authorization and access control schemes and requires a user to be authorized only once during a computer session.

The following is a more detailed example of how the above process may be implemented. Assume that the system 10 includes five authorization servers 16 and that a user logs into authorization server number 2 (AS2) with a browser. AS2 first creates a unique, random Session ID for the user such as 82012053249. The authorization server then creates a cookie named "SID" in the user's browser and assigns it a value of AS2.82012053249.

The authorization server 16 also creates an object in the directory 20 and relates it to the Session ID. The object is then populated with information from the user's profile, such as the user's ID, password, e-mail address, account number, etc.

The user is then offered a menu of applications/services that he or she is authorized to use or access. The user may select one of the applications or services,

for example a "View Bill" application. The View Bill application accesses the cookie named "SID" on the user's computer 12 and reads the value AS2.82012053249 from the cookie. The application then searches the directory 20 for the object associated with the cookie under the branch of the directory containing information for authorization server AS2. The application reads the associated attributes (i.e. the account number, user ID, password) from the directory to determine what information the user is authorized to access. The View Bill application may then collect authorized information such as billing information from one of the application servers 14 and present it to the user on the screen of the user's computer.

When the user logs off, the object for the user stored in the directory 20 is deleted. The object may be deleted immediately after log-off or after a certain amount of time has elapsed. If the user attempts to log-in after the object has been deleted, the above process may be repeated for the same or even a different authorization server.

Another possible application of the present invention is for on-line shopping carts. Assume, for example, that a user has already logged into the system 10 and that an object for the user has been created in the directory 20. Associated with the user's object is a shopping cart. The user browses shopping selections available via one or more merchandise servers and can add things to and or remove things from the shopping cart. If the user selects a book, for example, and indicates that he or she wants to purchase the book, the ISBN number of the book is added to the user's object in the directory. As the user purchases more items, these items are also added to the user's object in the directory.

When the user is ready to purchase the items, a check-out server queries the object in the directory 20 and obtains information for all of the items selected by the user. The check-out server may be a different server located in a different part of the network or may be connected with the other components in the network. The user information in the object may also contain credit card information so that purchases can be expedited. When the user logs out of the system 10, the user's object in the directory is preferably deleted to make room for objects for other users.

The present invention may also be used to determine how many users are logged into the system 10 at any given moment. Because a user object is created and maintained in the directory 20 whenever a user is logged into the system, a simple query to the directory can indicate how many users are currently logged into the system. For

example, the number of objects created under the AS2 branch of the directory indicates how many sessions were established by that particular authorization server. This information can be used to determine which authorization servers are over or under utilized.

Although the invention has been described with reference to the preferred embodiment illustrated in the attached drawing figures, it is noted that equivalents may be employed and substitutions made herein without departing from the scope of the invention as recited in the claims.

Having thus described the preferred embodiment of the invention, what is claimed as new and desired to be protected by Letters Patent includes the following:

CLAIMS:

1. A method for authenticating and authorizing computer users comprising the steps of:

a. storing security information for a plurality of computer users in a user profile database;

b. receiving at an authorization server coupled with the user profile database log-in information from a computer user who has launched a computer application;

c. in response to step b, creating a Session ID for the computer user with the authorization server;

d. storing at least a portion of the Session ID on the user's computer;

e. also in response to step b, creating an object associated with the computer user or the Session ID;

f. storing the object in a directory coupled with the authorization server;

g. copying at least some of the security information relating to the computer user from the user profile database to the object in the directory;

h. comparing the log-in information entered by the computer user to the security information for the computer user and allowing the computer user access to the launched computer application if the user is an authenticated or authorized user of the computer application; and

i. permitting other computer applications launched by the computer user to reference the Session ID on the user's computer so that the other computer applications may access the object for the computer user on the directory to authenticate or authorize the user for the other computer applications without requiring the user to re-enter the log-in information.

2. The method as set forth in claim 1, the security information including authentication and authorization information.

3. The method as set forth in claim 2, the authentication and authorization information including at least one of the following: user names, user IDs, passwords, public-key data, certificates, and access control information.

4. The method as set forth in claim1, the Session ID being based on at least one of the following: a date on which the computer user launched the computer application; a time in which the computer user launched the computer application; a TCP/IP address of the computer user; a user name of the computer user; and an account code.

5. The method as set forth in claim 1, further including the steps of creating a shopping cart and storing the shopping cart along with the object in the directory.

6. The method as set forth in claim 5, further including the steps of allowing the user to select items to be purchased and storing information relating to the selected items in the shopping cart.

7. A system for authenticating and authorizing computer users, the system comprising:

a user profile database for storing security information for a plurality of computer users;

an authorization server coupled with the user profile database for receiving log-in information from a computer user who has launched a computer application, for creating a Session ID for the computer user, for storing at least a portion of the Session ID on the user's computer and for creating an object associated with the computer user or the Session ID; and

a directory coupled with the authorization server for storing the object created by the authorization server; and

the authorization server being further operable for copying at least some of the security information relating to the computer user from the user profile database to the object in the directory, comparing log information entered by the computer user to the security information for the computer user and allowing the computer user access to the launched computer application if the user is an authenticated or authorized user of the computer application, permitting other computer applications launched by the computer user to reference the Session ID on the user's computer so that the other computer applications may access the object for the computer user on the directory to authenticate or authorize the user for the other computer applications without requiring the user to re-enter the log-in information.

8. The system as set forth in claim 7, the security information including authentication and authorization information.

9. The system as set forth in claim 8, the authentication and authorization information including at least one of the following: user names, user IDs, passwords, public-key data, certificates, and access control information.

10. The system as set forth in claim 7, the Session ID being based on at least one of the following: a date on which the computer user launched the computer application; a time in which the computer user launched the computer application; a TCP/IP address of the computer user; a user name of the computer user; and an account code.

11. The system as set forth in claim 7, the authorization server being further operable for creating a shopping cart and storing the shopping cart along with the object in the directory.

12. The system as set forth in claim 11, the authorization server being further operable for allowing the user to select items to be purchased and storing information relating to the selected items in the shopping cart.

ABSTRACT OF THE DISCLOSURE

A system and method for authenticating and authorizing computer users with a single, standard, directory-based set of applications. The invention combines dynamic directory services (DDS) with a directory access protocol such as the light weight directory access protocol (LDAP) to provide authentication and application-authorization for secured networks, applications, and programs. Dynamic information such as session information or user ID numbers is stored in a directory each time a user logs into the systems and is maintained in the directory until the user logs out. While the information exists in the directory, it can be queried by other programs, applications, or networks that use a directory service to authenticate or authorize the user for the program, application, or network.

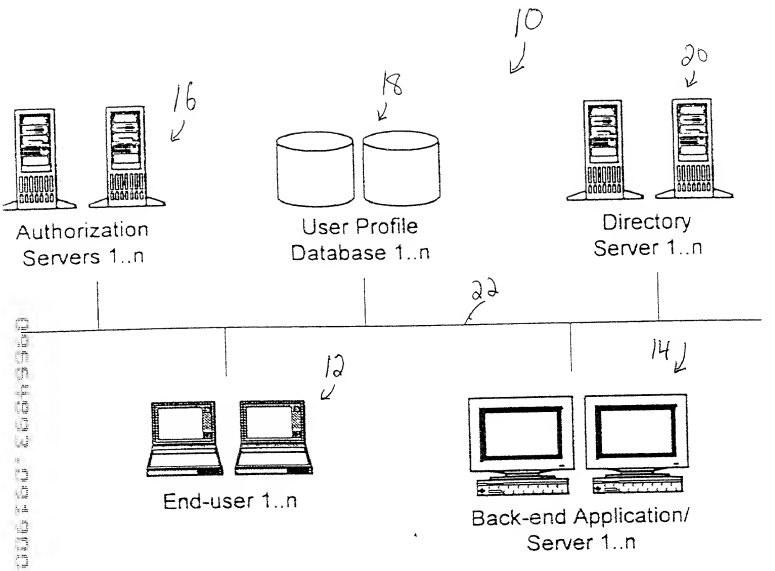
10
16
18
20
Authorization Servers 1..n
User Profile Database 1..n
Directory Server 1..n
22
12
14
End-user 1..n
Back-end Application/ Server 1..n

Fig. 1

Practitioner's Docket No. 30604 *PATENT*

COMBINED DECLARATION AND POWER OF ATTORNEY

(ORIGINAL, DESIGN, NATIONAL STAGE OF PCT, SUPPLEMENTAL, DIVISIONAL, CONTINUATION, OR C-I-P)

As a below named inventor, I hereby declare that:

TYPE OF DECLARATION

This declaration is of the following type:

(check one applicable item below)

[X] original.
[ ] design.
[ ] supplemental.

NOTE: If the declaration is for an International Application being filed as a divisional, continuation or continuation-in-part application, do not check next item; check appropriate one of last three items.

[ ] national stage of PCT.

NOTE. If one of the following 3 items apply, then complete and also attach ADDED PAGES FOR DIVISIONAL, CONTINUATION OR C-I-P.

NOTE: See 37 C.F.R. § 1.63(d) (continued prosecution application) for use of a prior nonprovisional application declaration in the continuation or divisional application being filed on behalf of the same or fewer of the inventors named in the prior application.

[ ] divisional.
[ ] continuation.

NOTE: Where an application discloses and claims subject matter not disclosed in the prior application, or a continuation or divisional application names an inventor not named in the prior application, a continuation-in-part application must be filed under 37 C.F.R. § 1.53(b) (application filing requirements-nonprovisional application).

[ ] continuation-in-part (C-I-P).

INVENTORSHIP IDENTIFICATION

WARNING: *If the inventors are each not the inventors of all the claims, an explanation of the facts, including the ownership of all the claims at the time the last claimed invention was made, should be submitted.*

My residence, post office address and citizenship are as stated below, next to my name. I believe that I am the original, first and sole inventor *(if only one name is listed below)* or an original, first and joint inventor

(if plural names are listed below) of the subject matter that is claimed, and for which a patent is sought on the invention entitled:

TITLE OF INVENTION

AUTHENTICATION, APPLICATION-AUTHORIZATION, AND USER PROFILING USING DYNAMIC DIRECTORY SERVICES

SPECIFICATION IDENTIFICATION

The specification of which:

(complete (a), (b), or (c))

(a) [X] is attached hereto.

NOTE: "The following combinations of information supplied in an oath or declaration filed on the application filing date with a specification are acceptable as minimums for identifying a specification and compliance with any one of the items below will be accepted as complying with the identification requirement of 37 C.F.R. § 1.63:

"(1) name of inventor(s), and reference to an attached specification which is both attached to the oath or declaration at the time of execution and submitted with the oath or declaration on filing;

"(2) name of inventor(s), and attorney docket number which was on the specification as filed; or

"(3) name of inventor(s), and title which was on the specification as filed."

Notice of July 13, 1995 (1177 O.G. 60).

(b) [ ] was filed on _____, as [ ] Application No. 0 / _____ or
[ ] _____ and was amended on _____ *(if applicable)*.

NOTE Amendments filed after the original papers are deposited with the PTO that contain new matter are not accorded a filing date by being referred to in the declaration. Accordingly, the amendments involved are those filed with the application papers or, in the case of a supplemental declaration, are those amendments claiming matter not encompassed in the original statement of invention or claims. See 37 C.F.R. § 1.67.

NOTE: "The following combinations of information supplied in an oath or declaration filed after the filing date are acceptable as minimums for identifying a specification and compliance with any one of the items below will be accepted as complying with the identification requirement of 37 C.F.R. § 1.63:

"(1) name of inventor(s), and application number (consisting of the series code and the serial number; e.g.,08/123,456);

"(2) name of inventor(s), serial number and filing date;

"(3) name of inventor(s) and attorney docket number which was on the specification as filed;

"(4) name of inventor(s), title which was on the specification as filed and filing date;

"(5) name of inventor(s), title which was on the specification as filed and reference to an attached specification which is both attached to the oath or declaration at the time of execution and submitted with the oath or declaration; or

"(6) name of inventor(s), title which was on the specification as filed and accompanied by a cover letter accurately identifying the application for which it was intended by either the application number (consisting of the series code and the serial number; e.g.,08/123,456), or serial number and filing date. Absent any statement(s) to the contrary, it will be presumed that the application filed in the PTO is the application which the inventor(s) executed by signing the oath or declaration."

Notice of July 13, 1995 (1177 O.G. 60), M.P.E.P. § 601(a), 6th ed., rev.3.

(c) [ ] was described and claimed in PCT International Application No. _____ filed on _____ and as amended under PCT Article 19 on _____ *(if any)*.

SUPPLEMENTAL DECLARATION (37 C.F.R. § 1.67(b))

(complete the following where a supplemental declaration is being submitted)

[ ] I hereby declare that the subject matter of the

[ ] attached amendment
[ ] amendment filed on _____.

was part of my/our invention and was invented before the filing date of the original application, above identified, for such invention.

ACKNOWLEDGMENT OF REVIEW OF PAPERS AND DUTY OF CANDOR

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information, which is material to patentability as defined in 37, Code of Federal Regulations, § 1.56,

(also check the following items, if desired)

[ ] and which is material to the examination of this application, namely, information where there is a substantial likelihood that a reasonable Examiner would consider it important in deciding whether to allow the application to issue as a patent, and

[ ] in compliance with this duty, there is attached an information disclosure statement, in accordance with 37 C.F.R. § 1.98.

PRIORITY CLAIM (35 U.S.C. § 119(a)-(d))

NOTE: "The claim to priority need be in no special form and may be made by the attorney or agent if the foreign application is referred to in the oath or declaration as required by § 1.63. The claim for priority and the certified copy of the foreign application specified in 35 U.S.C. § 119(b) must be filed in the case of an interference (§ 1.630), when necessary to overcome the date of a reference relied upon by the examiner, when specifically required by the examiner, and in all other situations, before the patent is granted. If the claim for priority or the certified copy of the foreign application is filed after the date the issue fee is paid, it must be accompanied by a petition requesting entry and by the fee set forth in § 1.17(i). If the certified copy is not in the English language, a translation need not be filed except in the case of interference; or when necessary to overcome the date of a reference relied upon by the examiner; or when specifically required by the examiner, in which event an English language translation must be filed together with a statement that the translation of the certified copy is accurate." 37 C.F.R. § 1.55(a).

I hereby claim foreign priority benefits under Title 35, United States Code, § 119(a)-(d) of any foreign application(s) for patent or inventor's certificate or of any PCT international application(s) designating at least one country other than the United States of America listed below and have also identified below any foreign application(s) for patent or inventor's certificate or any PCT international application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application(s) of which priority is claimed.

(complete (d) or (e))

(d) [X] no such applications have been filed.
(e) [ ] such applications have been filed as follows.

NOTE: Where item (c) is entered above and the International Application which designated the U.S. itself claimed priority check item (e), enter the details below and make the priority claim.

PRIOR FOREIGN/PCT APPLICATION(S) FILED WITHIN 12 MONTHS (6 MONTHS FOR DESIGN) PRIOR TO THIS APPLICATION AND ANY PRIORITY CLAIMS UNDER 35 U.S.C. § 119(a)-(d)

COUNTRY (OR INDICATE IF PCT)	APPLICATION NUMBER	DATE OF FILING DAY, **MONTH**, YEAR	PRIORITY CLAIMED UNDER 35 USC 119
			[ ]YES [ ]NO
			[ ]YES [ ]NO
			[ ]YES [ ]NO
			[ ]YES [ ]NO
			[ ]YES [ ]NO

CLAIM FOR BENEFIT OF PRIOR U.S. PROVISIONAL APPLICATION(S)
(35 U.S.C. § 119(e))

I hereby claim the benefit under Title 35, United States Code, § 119(e) of any United States provisional application(s) listed below:

PROVISIONAL APPLICATION NUMBER	FILING DATE
_____/_____	_____
_____/_____	_____
_____/_____	_____

CLAIM FOR BENEFIT OF EARLIER U.S./PCT APPLICATION(S) UNDER 35 U.S.C. § 120

[ ] The claim for the benefit of any such applications are set forth in the attached ADDED PAGES TO COMBINED DECLARATION AND POWER OF ATTORNEY FOR DIVISIONAL, CONTINUATION OR CONTINUATION-IN-PART (C-I-P) APPLICATION.

ALL FOREIGN APPLICATION(S), *IF ANY*, FILED MORE THAN 12 MONTHS (6 MONTHS FOR DESIGN) PRIOR TO THIS U.S. APPLICATION

_____

_____

_____

NOTE: If the application filed more than 12 months from the filing date of this application is a PCT filing forming the basis for this application entering the United States as (1) the national stage, or (2) a continuation, divisional, or continuation-in-part, then also complete ADDED PAGES TO COMBINED DECLARATION AND POWER OF ATTORNEY FOR DIVISIONAL, CONTINUATION OR C-I-P APPLICATION for benefit of the prior U.S. or PCT application(s) under 35 U.S.C § 120.

POWER OF ATTORNEY

I hereby appoint the following practitioner(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith.

Robert D. Hovey	19,223	Andrew G. Colombo	40,565
Warren N. Williams	19,156	Scott R. Brown	40,535
Stephen D. Timmons	26,513	Tracy L. Bornman	42,347
John M. Collins	26,262	Tracey S. Truitt	43,205
Thomas H. Van Hoozer	32,761	Harley R. Ball	31,733
Thomas B. Luebbering	37,874	Steven J. Funk	35,875

(Check the following item, if applicable)

[ ] I hereby appoint the practitioner(s) associated with the Customer Number provided below to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith.

[ ] Attached, as part of this declaration and power of attorney, is the authorization of the above-named practitioner(s) to accept and follow instructions from my representative(s).

SEND CORRESPONDENCE TO
THOMAS B. LUEBBERING

DIRECT TELEPHONE CALLS TO:
(Name and telephone number)

[X] Address

THOMAS B. LUEBBERING
(816)474-9050

Attn: THOMAS B. LUEBBERING
HOVEY, WILLIAMS, TIMMONS & COLLINS
2405 Grand Boulevard, Suite 400
Kansas City, MO 64108-2519

[ ] Customer Number _____

DECLARATION

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

SIGNATURE(S)

NOTE: Carefully indicate the family (or last) name, as it should appear on the filing receipt and all other document

NOTE: Each inventor must be identified by full name, including the family name, and at least one given name without abbreviation together with any other given name or initial, and by his/her residence, post office address and country of citizenship. 37 C.F.R § 1.63(a)(3).

NOTE: Inventors may execute separate declarations/oaths provided <u>each</u> declaration/oath sets forth all the inventors Section 1.63(a)(3) requires that a declaration/oath, inter alia, identify each inventor and prohibits the execution of separate declarations/oaths which each sets forth only the name of the executing inventor. 62 Fed. Reg. 53,131, 53,142, October 10, 1997.

Full name of sole or first inventor

John *(Given Name)* MICHAEL *(Middle Initial or Name)* Everson *Family (Or Last Name)*

Inventor's signature _____

Date 9-12-00 **Country of Citizenship** United States of America

Residence 11720 Troost Avenue, Kansas City, MO 64131

Post Office Address 11720 Troost Avenue, Kansas City, MO 64131

■■■■■■

Full name of second joint inventor, if any

James *(Given Name)* W. *(Middle Initial or Name)* Norris *Family (Or Last Name)*

Inventor's signature _____

Date 9-12-00 **Country of Citizenship** United States of America

Residence 9935 North Harrison, Kansas City, MO 64155

Post Office Address 9935 North Harrison, Kansas City, MO 64155

■■■■■■

Full name of third joint inventor, if any

(Given Name) *(Middle Initial or Name)* *Family (Or Last Name)*

Inventor's signature _____

Date _____ **Country of Citizenship** _____

Residence _____

Post Office Address _____

(check proper box(es) for any of the following added page(s) that form a part of this declaration)

[ ] **Signature** for fourth and subsequent joint inventors. *Number of pages added* _____

* * *

[ ] **Signature** by administrator(trix), executor(trix) or legal representative for deceased or incapacitated inventor. *Number of pages added* _____

* * *

[ ] **Signature** for inventor who refuses to sign or cannot be reached by person authorized under 37 C.F.R. § 1.47. *Number of pages added* _____

* * *

[ ] Added page for **signature** by one joint inventor on behalf of deceased inventor(s) where legal representative cannot be appointed in time. (37 C.F.R. § 1.47)

* * *

[ ] Added pages to combined declaration and power of attorney for divisional, continuation, or continuation-in-part (C-I-P) application.

[ ] Number of pages added _____

* * *

[ ] Authorization of practitioner(s) to accept and follow instructions from representative.

(If no further pages form a part of this Declaration, then end this Declaration with this page and check the following item)

[X] This declaration ends with this page.